



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/500,820	07/07/2004	Masahiro Oho	2004-1067A	8282
52349	7590	06/09/2009	EXAMINER	
WENDEROTH, LIND & PONACK L.L.P.			FEARER, MARK D	
1030 15th Street, N.W.				
Suite 400 East			ART UNIT	PAPER NUMBER
Washington, DC 20005-1503			2443	
			MAIL DATE	DELIVERY MODE
			06/09/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/500,820	OHO ET AL.	
	Examiner	Art Unit	
	MARK D. FEARER	2443	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 09 March 2009.
 2a) This action is **FINAL**. 2b) This action is non-final.
 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-8, 10-21 and 23-29 is/are pending in the application.
 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
 5) Claim(s) _____ is/are allowed.
 6) Claim(s) 1-4, 7, 10-12, 14-16, 18-21 and 23-29 is/are rejected.
 7) Claim(s) 5-6, 8, 13, and 17 is/are objected to.
 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
 10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ . |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____. | 6) <input type="checkbox"/> Other: _____ . |

DETAILED ACTION

1. Applicant's Request for Continued Examination filed 08 April 2009 is acknowledged.
2. Applicant's Amendment filed 09 March 2009 is acknowledged.
3. Claims 1-8 and 10-21, and 23-29 have been amended.
4. Claim 22 has been cancelled.
5. Claims 1-8, 10-21, and 23-29 are pending in the present application.

Continued Examination Under 37 CFR 1.114

6. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114.

Allowable Subject Matter

7. Claims 5-6, 8, 13, and 17 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

The factual inquiries set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

9. Claims 1-2, 4, 7, 10-11, 14-15, 18-20, 23 and 27-29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Franklin et al. (US 6263436 B1) in view of Boykin et al. (US 20030079222 A1) and in further view of Stefik et al. (US 5629980 A).

Consider claim 1. Franklin et al. clearly discloses a unit-to-unit data exchange system for exchanging data between units connected to each other via a communication medium, the unit-to-unit data exchange system comprising: a first unit having at least one piece of data that can be exchanged and requesting to exchange data with another unit; a second unit having data of interest to the first unit; and an exchange completion data keeping device connected to the first and second units via the communications medium for keeping first exchange completion data that is a description key, and that is necessary, after completion of the data exchange between the first and second units, for reproducing data obtained by the first unit and second exchange completion data that is necessary, after completion of the data exchange between the first and second units, for reproducing data obtained by the second unit, wherein the exchange completion data keeping device includes exchange completion data transmission means for transmitting the first exchange completion data to the first unit and the second exchange completion data to the second unit only when the first and second units have successfully received data of interest (column 3 lines 16-37).

However, Franklin et al. fails to disclose fails to disclose an exchange device that transmits a decryption key to the first unit, that the first unit transmits, to the second unit, the entire encrypted content data of interest and the second unit transmits, to the first

unit, the entire encrypted content data of interest, or that the exchange device transmits the decryption keys, when the first unit has successfully received the encrypted content data of interest to the first unit and the second unit has successfully received the encrypted content data of interest to the second unit.

Boykin et al. discloses a system and method for distributing perceptually encrypted encoded files of music and movies wherein an exchange device transmits a conditional decryption key to a first video sub-packet (read as a first unit), that the first unit transmits, to a second video sub-packet (read as a second unit), the entire encrypted content data of interest and the second unit transmits, to the first unit, the entire encrypted content data of interest, and the exchange device transmits the decryption keys, when the first unit has successfully received the encrypted content data of interest to the first unit and the second unit has successfully received the encrypted content data of interest to the second unit ((“Referring to FIG. 2 in conjunction with FIG. 1 the modulated data is then sent through a digital satellite 8 directly to a digital signal receiving apparatus installed in a contract user's household, i.e., a terminal 10, or sent through the digital satellite 8 to a signal distributing station 9 which is called a head end. The data, transmitted to the signal distributing station 9, is sent to the terminal 10 via cable. In the terminal 10, when the transmission data is directly sent via the satellite 8, the data is received by an antenna 11 and sent to a front end section 12. When the transmission data is sent from the signal distributing station 9 via the cable, it is inputted directly to the front end section 12. A user contracts with the broadcasting station 1 and accesses a key which is authorized to each user to the terminal 10, with

respect to the transmission data sent directly from the satellite 8 or from the satellite 8 via the signal distributing station 9, so that the user is authorized as a contract user and bill processing is performed, and at the same time, the user can appreciate desired software information. In the terminal 10 the transmission data is processed by the front end section 12 which includes a tuner, a demodulator and an error corrector. The processed data is input to a data fetch section 13. In the data fetch section 13, the multiplexed data is demultiplexed by the demultiplexer 14. The data is separated into a video signal, an audio signal, and data other than these signals. In a decryption section 15, ciphers are decrypted while performing bill processing. In a packet separation section 16, the decrypted data is packet separated. Compression of the data is expanded by an MPEG decoder 17. The video and audio signals are digital-to-analog converted to analog signals and are outputs to a television. When fee-charged software information, such as video on demand or near video on demand is transmitted, a digital storage 18 such as tape media or disk media is incorporated into or connected to the terminal 10 to meet the convenience of users and to effectively utilize a digital transmission path. Large amounts of software data have been downloaded to the storage 18 by making use of an unoccupied time band and an unoccupied transmission path. When the user looks at the software information at hand, the user accesses it with a smart card to perform bill processing, and reproduction limitation is lifted. If the user accesses a central processing unit by means of the smart card 19 and a modem 21. The CPU 20 performs an inquiry of registration to an authorization center 22 through the modem 21. The authorization center 22 confirms registration by means of a conditional

access 23. If registration is confirmed, the authorization center 22 performs bill processing and also performs notification of confirmation to the CPU 20 through the modem 21. The CPU 20 sends the decryption key to a local conditional access 24 by this notification. The local conditional access 24 decrypts a cipher which has been put over the data recorded on the storage 18. The reproduction limitation is lifted and the packet of the data recorded on the storage 18 is separated by the packet separation section 16. The compression of the packet-separated data is decompressed (expanded) by the MPEG decoder 17 and then the expanded data is digital-to-analog converted to be output to television as the analog signal and audio signal A/V. If, in the security system in a current broadcasting form, software information has been downloaded to the storage 18 to try to realize a system where this software can be appreciated when user wants to see it, then the following problems will arise.") paragraph 0125 ("Referring to FIG. 37 in conjunction with FIG. 36 the encoding strategy consists in separating the spectral information contained in the video sequence across a first video sub-packet 741 and a second video sub-packet 742. The second video sub-packet 742 containing the refinement (high frequency) data is encrypted. To a decoder the non -encrypted first video sub-packet 741 will appear as the original video packet 713. The encrypted second video sub-packet 742 is inserted in the stream as padding data. This operation can be performed both in the luminance as well as in the chrominance domain in order to generate a variety of encoded sequences with different properties. It is possible to build a video sequence where the basic low-fidelity mode gives access to a low-resolution version of the video sequence. The user is granted access to the full-

resolution version when he purchases the key. Perceptual encryption is applicable to most video encoding standards, since most of them are based on separation of the color components (RGB or YCbCr) and use spectral information to achieve high compression rates. Perceptual encryption allows simultaneous content protection and preview capabilities. It is safer than watermarking since it prevents intellectual property rights infringement rather than trying to detect it after the fact. Perceptual encryption is applied to video encoded under the MPEG-1 compression standard. The use of perceptual encryption is not limited to this specific standard. It is applicable to a large ensemble of audio/video compression standards, including MPEG-2, MPEG4, MPEG-21, MPEG-7, QuickTime, Real Time, AVI, Cine Pak and others.”) paragraph 0175).

Franklin et al. discloses a prior art unit-to-unit data exchange system for exchanging data between units connected to each other via a communication medium, the unit-to-unit data exchange system comprising: a first unit having at least one piece of data that can be exchanged and requesting to exchange data with another unit; a second unit having data of interest to the first unit; and an exchange completion data keeping device connected to the first and second units via the communications medium for keeping first exchange completion data that is a description key, and that is necessary, after completion of the data exchange between the first and second units, for reproducing data obtained by the first unit and second exchange completion data that is necessary, after completion of the data exchange between the first and second units, for reproducing data obtained by the second unit, wherein the exchange completion data keeping device includes exchange completion data transmission

means for transmitting the first exchange completion data to the first unit and the second exchange completion data to the second unit only when the first and second units have successfully received data of interest upon which the claimed invention can be seen as an improvement.

Boykin et al. teaches a prior art comparable system and method for distributing perceptually encrypted encoded files of music and movies wherein an exchange device transmits a conditional decryption key to a first video sub-packet, that the first unit transmits, to a second video sub-packet, the entire encrypted content data of interest and the second unit transmits, to the first unit, the entire encrypted content data of interest, and the exchange device transmits the decryption keys, when the first unit has successfully received the encrypted content data of interest to the first unit and the second unit has successfully received the encrypted content data of interest to the second unit.

Thus, the manner of enhancing a particular device (system and method for distributing perceptually encrypted encoded files of music and movies wherein an exchange device transmits a conditional decryption key to a first video sub-packet (read as a first unit), that the first unit transmits, to a second video sub-packet (read as a second unit), the entire encrypted content data of interest and the second unit transmits, to the first unit, the entire encrypted content data of interest, and the exchange device transmits the decryption keys, when the first unit has successfully received the encrypted content data of interest to the first unit and the second unit has successfully received the encrypted content data of interest to the second unit) was made part of the

ordinary capabilities of one skilled in the art based upon the teaching of such improvement in Boykin et al. Accordingly, one of ordinary skill in the art would have been capable of applying this known improvement technique in the same manner to the prior art unit-to-unit data exchange system for exchanging data between units connected to each other via a communication medium, the unit-to-unit data exchange system comprising: a first unit having at least one piece of data that can be exchanged and requesting to exchange data with another unit; a second unit having data of interest to the first unit; and an exchange completion data keeping device connected to the first and second units via the communications medium for keeping first exchange completion data that is a description key, and that is necessary, after completion of the data exchange between the first and second units, for reproducing data obtained by the first unit and second exchange completion data that is necessary, after completion of the data exchange between the first and second units, for reproducing data obtained by the second unit, wherein the exchange completion data keeping device includes exchange completion data transmission means for transmitting the first exchange completion data to the first unit and the second exchange completion data to the second unit only when the first and second units have successfully received data of interest of Franklin et al. and the results would have been predictable to one of ordinary skill in the art, namely, one skilled in the art would have readily recognized a secure gateway.

However, Franklin et al., as modified by Boykin et al., fails to disclose a system or method wherein the exchange completion data keeping~ device receives a first communication result from the first unit when a first communication section between the

first unit and the second unit is terminated, and receives a second communication result from the second unit when a second communication section between the first unit and the second unit is terminated, wherein the exchange completion data keeping device determines whether the first unit has successfully received from the second unit the encrypted second content data of interest to the first unit based on the first communication result, and determines whether the second unit has successfully received from the first unit the encrypted first content data of interest to the second unit based on the second communication result.

Stefik et al. discloses a system for controlling the distribution and use of digital works wherein the exchange completion data keeping device receives a first communication result from the first unit when a first communication section between the first unit and the second unit is terminated, and receives a second communication result from the second unit when a second communication section between the first unit and the second unit is terminated, wherein the exchange completion data keeping device determines whether the first unit has successfully received from the second unit the encrypted second content data of interest to the first unit based on the first communication result, and determines whether the second unit has successfully received from the first unit the encrypted first content data of interest to the second unit based on the second communication result ((“..if said first repository and said second repository each successfully complete said set of registration steps, said first and second repository exchanging session encryption and decryption keys for secure

transmission of subsequent communications between said first and second repository; ..") column 54 lines 27-32).

Franklin et al., as modified by Boykin et al., discloses a prior art system and method for distributing perceptually encrypted encoded files of music and movies wherein an exchange device transmits a conditional decryption key to a first video sub-packet, that the first unit transmits, to a second video sub-packet (read as a second unit), the entire encrypted content data of interest and the second unit transmits, to the first unit, the entire encrypted content data of interest, and the exchange device transmits the decryption keys, when the first unit has successfully received the encrypted content data of interest to the first unit and the second unit has successfully received the encrypted content data of interest to the second unit, and unit-to-unit data exchange system for exchanging data between units connected to each other via a communication medium, the unit-to-unit data exchange system comprising: a first unit having at least one piece of data that can be exchanged and requesting to exchange data with another unit; a second unit having data of interest to the first unit; and an exchange completion data keeping device connected to the first and second units via the communications medium for keeping first exchange completion data that is a description key, and that is necessary, after completion of the data exchange between the first and second units, for reproducing data obtained by the first unit and second exchange completion data that is necessary, after completion of the data exchange between the first and second units, for reproducing data obtained by the second unit, wherein the exchange completion data keeping device includes exchange completion

data transmission means for transmitting the first exchange completion data to the first unit and the second exchange completion data to the second unit only when the first and second units have successfully received data upon which the claimed invention can be seen as an improvement.

Stefik et al. teaches a prior art comparable system for controlling the distribution and use of digital works wherein the exchange completion data keeping device receives a first communication result from the first unit when a first communication section between the first unit and the second unit is terminated, and receives a second communication result from the second unit when a second communication section between the first unit and the second unit is terminated, wherein the exchange completion data keeping device determines whether the first unit has successfully received from the second unit the encrypted second content data of interest to the first unit based on the first communication result, and determines whether the second unit has successfully received from the first unit the encrypted first content data of interest to the second unit based on the second communication result.

Thus, the manner of enhancing a particular device (system for controlling the distribution and use of digital works wherein the exchange completion data keeping device receives a first communication result from the first unit when a first communication section between the first unit and the second unit is terminated, and receives a second communication result from the second unit when a second communication section between the first unit and the second unit is terminated, wherein the exchange completion data keeping device determines whether the first unit has

successfully received from the second unit the encrypted second content data of interest to the first unit based on the first communication result, and determines whether the second unit has successfully received from the first unit the encrypted first content data of interest to the second unit based on the second communication result) was made part of the ordinary capabilities of one skilled in the art based upon the teaching of such improvement in Stefik et al. Accordingly, one of ordinary skill in the art would have been capable of applying this known improvement technique in the same manner to the prior art system and method for distributing perceptually encrypted encoded files of music and movies wherein an exchange device transmits a conditional decryption key to a first video sub-packet, that the first unit transmits, to a second video sub-packet (read as a second unit), the entire encrypted content data of interest and the second unit transmits, to the first unit, the entire encrypted content data of interest, and the exchange device transmits the decryption keys, when the first unit has successfully received the encrypted content data of interest to the first unit and the second unit has successfully received the encrypted content data of interest to the second unit, and unit-to-unit data exchange system for exchanging data between units connected to each other via a communication medium, the unit-to-unit data exchange system comprising: a first unit having at least one piece of data that can be exchanged and requesting to exchange data with another unit; a second unit having data of interest to the first unit; and an exchange completion data keeping device connected to the first and second units via the communications medium for keeping first exchange completion data that is a description key, and that is necessary, after completion of the data exchange between

the first and second units, for reproducing data obtained by the first unit and second exchange completion data that is necessary, after completion of the data exchange between the first and second units, for reproducing data obtained by the second unit, wherein the exchange completion data keeping device includes exchange completion data transmission means for transmitting the first exchange completion data to the first unit and the second exchange completion data to the second unit only when the first and second units have successfully received data of Franklin et al., as modified by Boykin et al., and the results would have been predictable to one of ordinary skill in the art, namely, one skilled in the art would have readily recognized a system and method of an encryption gateway.

Consider claim 2, as applied to claim 1. Franklin et al., as modified by Boykin et al. and Stefik et al., discloses a unit-to-unit data exchange system: wherein the first unit includes: first exchange completion data production means for producing the second exchange completion data; and first exchange completion data transmission means for transmitting the second exchange completion data produced by the first exchange completion data production means to the exchange completion data keeping device; wherein the second unit includes: second exchange completion data production means for producing the first exchange completion data; and second exchange completion data transmission means for transmitting the first exchange completion data produced by the second exchange completion data production means to the exchange completion data keeping device; and wherein the exchange completion data keeping device further

includes exchange completion data keeping means for keeping the first exchange completion data transmitted from the second exchange completion data transmission means and the second exchange completion data transmitted from the exchange completion data transmission means, such that the first unit from which the exchange completion data has been transmitted can be identified and the second unit, from which the first exchange completion data has been transmitted, can be identified (Franklin et al., column 6 lines 26-34 column and 8 lines 20-44 and column 3 lines 1-15).

Consider claim 4, as applied to claim 1. Franklin et al., as modified by Boykin et al. and Stezik et al., discloses a unit-to-unit data exchange system: wherein the first unit further includes first exchange completion data production requesting means for requesting the exchange completion data keeping device to produce the second exchange completion data; the second unit further includes second exchange completion data production requesting means for requesting the exchange completion data keeping device to produce the first exchange completion data; and the exchange completion data keeping device further includes: exchange completion data production means for producing the first exchange completion data in response to the request from the first exchange completion data production requesting means and for producing the second exchange completion data in response to the request from the second exchange completion data production requesting means; and exchange completion data keeping means for keeping the first exchange completion data and the second exchange completion data produced by the exchange completion data production

means so that the first unit and the second unit can be respectfully identified (Franklin et al., column 6 lines 34-43).

Consider claim 7, as applied to claim 1. Franklin et al., as modified by Boykin et al. and Stefik et al., discloses a unit-to-unit data exchange system wherein: each of the first and second units further includes communication result notification means for notifying the exchange completion data keeping device of a communication result when a communication session with another of the first and second units is terminated; and the exchange completion data transmission means determines whether or not the first unit and the second unit have successfully received the respective encrypted content data of interest based on the communication results from the communication result notification means of the first unit and the second unit (Franklin et al., claim 13); the first unit further includes a first communication result notification unit for notifying the exchange completion data keeping device of the first communication result when the first communication session is terminated ((“Assuming that the repository is not on the hotlist, the repository identification needs to be verified. In other words, repository-2 needs to validate that the repository on the other end is really repository-1. This is termed performance testing and is performed in order to avoid invalid access to the repository via a counterfeit repository replaying a recording of a prior session initiation between repository-1 and repository-2. Performance testing is initiated by repository-2 generating a performance message, step 1609. The performance message consists of a nonce, the names of the respective repositories, the time and the registration identifier

received from repository-1. A nonce is a generated message based on some random and variable information (e.g. the time or the temperature.) The nonce is used to check whether repository-1 can actually exhibit correct encrypting of a message using the private keys it claims to have, on a message that it has never seen before. The performance message is encrypted using the public key specified in the registration message of repository-1. The performance message is transmitted to repository-1, step 1610, where it is decrypted by repository-1 using its private key, step 1611. Repository-1 then checks to make sure that the names of the two repositories are correct, step 1612, that the time is accurate, step 1613 and that the registration identifier corresponds to the one it sent, step 1614. If any of these tests fails, the transaction is terminated per step 1616. Assuming that the tests are passed, repository-1 transmits the nonce to repository-2 in the clear, step 1615. Repository-2 then compares the received nonce to the original nonce, step 1617. If they are not identical, the registration transaction terminates in an error per step 1618. If they are the same, the registration transaction has successfully completed.") Stefik et al., column 28 lines 32-63).

Consider claim 10, as applied to claim 1. Franklin et al., as modified by Boykin et al. and Stefik et al., discloses a unit-to-unit data exchange system according to claim 1, wherein each of the first unit and the second unit further include resend requesting means for requesting another of the first and second units to resend the respective encrypted content data of interest if the respective unit fails to fully receive the

respective encrypted content data of interest from the other of the first unit and second unit (Franklin et al., column 7 55-63).

Consider claim 11. Franklin et al., as modified by Boykin et al. and Stefik et al., discloses a unit for exchanging content data owned by the unit with content data of interest to the unit that that is owned by another unit, wherein the unit and the other unit encrypt the content data owned thereby, respectively, when the respective content data is exchanged therebetween, wherein the unit comprises exchange completion data production means for producing first exchange completion data that is a decryption key, and that is necessary for reproducing the encrypted content data that is obtained by encrypting the content data owned by the unit; exchange completion data registration means for registering the first exchange completion data produced by the exchange completion data production means at an exchange completion data keeping device for keeping exchange completion data; and exchange completion data obtaining means for obtaining, from the exchange completion data keeping device, second exchange completion data that is a decryption key, and that is necessary for reproducing encrypted content data obtained from the other unit when a communication session with the other unit is terminated, and wherein the exchange completion data keeping device transmits (i) the first exchange completion data to the other unit, and (ii) the second exchange completion data to the unit, the transmission of the first and second exchange completion data being performed only when the unit and the other unit have

successfully received encrypted content data of interest (Franklin et al., column 6 lines 26-34 column and 8 lines 20-44 and column 8 lines 1-8).

Consider claims 14 and 18, as applied to claims 11 and 15, respectively. Franklin et al., as modified by Boykin et al. and Stefik et al., discloses a unit comprising resend requesting means for requesting the other unit to resend encrypted content data of interest to the unit if the unit fails to fully receive the encrypted content data of interest to the unit (Franklin et al., column 10 lines 36-45).

Consider claim 15. Franklin et al., as modified by Boykin et al. and Stefik et al., discloses a unit for exchanging content data owned by the unit with content data of interest to the unit that is owned by another unit, wherein the unit and the other unit encrypt the content data owned thereby, respectively, when the respective content data is exchanged therebetween, wherein the unit comprises: exchange completion data production requesting means for requesting an exchange completion data keeping device for keeping exchange completion data to produce first exchange completion data that is a decryption key, and that is necessary for reproducing encrypted content data of interest to the other unit that is obtained by encrypting the content data owned by the unit; and exchange completion data obtaining means for obtaining, from the exchange completion data keeping device, second exchange completion data that is a decryption key, and that is necessary for reproducing encrypted content data obtained from the

other unit when a communication session with the other unit is terminated, and wherein the exchange completion data keeping device transmits (i) the first exchange completion data to the other unit, and (ii) the second exchange completion data to the unit, the transmission of the first and second exchange completion data being performed only when the unit and the other unit have successfully received encrypted content data of interest (Franklin et al., column 6 lines 26-34 column and 8 lines 20-44 and column 8 lines 1-8); and exchange completion data keeping device storing the first exchange completion data and when the other unit has successfully received the encrypted first content data of interest (Stefik et al., column 54 lines 27-32).

Consider claim 19. Franklin et al., as modified by Boykin et al. and Stefik et al., discloses an exchange completion data keeping device used in a system for exchanging content data between a first unit and a second unit connected to each other via a communication medium, the first unit storing first content data of interest to the second unit and encrypting the first content data of interest, the second unit storing second content data of interest to the first unit and encrypting the second content data of interest, the exchange completion data keeping device comprising: an exchange completion data keeping means unit for storing (i) first exchange completion data that is a decryption key and that is necessary for reproducing encrypted second content data of interest to the first unit that is obtained by the first unit from the second unit and (ii) second exchange completion data that is a decryption key and that is necessary for reproducing encrypted first content data of interest to the second unit that is obtained by

the second unit from the first unit; and a data reception unit for receiving a first communication result from the first unit when a first communication section between the first unit and the second unit is terminated, and receives a second communication result from the second unit when a second communication section between the first unit and the second unit is terminated; a determination unit for determining whether the first unit has successfully received from the second unit the encrypted second content data of interest to the first unit based on the first communication result, and determines whether the second unit has successfully received from the first unit the encrypted first content data of interest to the second unit based on the second communication result; and an exchange completion data transmission means unit for transmitting (i) the first exchange completion data to the first unit and (ii) the second exchange completion data to the second unit~ only when the first unit and has successfully received from the second unit the encrypted second content data of interest to the first unit and when the second unit has successfully received from the first unit the encrypted first content data of interest to the second unit (Franklin et al., column 2 lines 63-67 and column 3 lines 1-15, and Stefik et al., column 54 lines 27-32).

Consider claim 20, as applied to claim 19. Franklin et al., as modified by Boykin et al. and Stefik et al., discloses an exchange completion data keeping device according to claim 19, further comprising: exchange completion data production means for producing the exchange completion data in response to a request from the first unit and the second unit; and exchange completion data keeping means for keeping the

exchange completion data produced by the exchange completion data production means so that the first unit and the second unit can be identified. (Franklin et al., column 6 lines 26-34 column and 8 lines 20-44 and column 10 lines 36-45); and the second exchange completion data in response to a request from the second unit (Stefik et al., column 54 lines 27-32)

Consider claim 23, as applied to claim 22. Franklin et al., as modified by Boykin et al. and Stefik et al., discloses an exchange completion data keeping device according to claim 22, wherein: the communication result is information indicating whether or not the encrypted content data of interest has been received successfully; and the exchange completion data transmission means transmits exchange completion data when receiving information indicating that the encrypted content data has been received successfully from the first and second units (Franklin et al., column 11 lines 55-67 and column 12 lines 1-15); the first communication result indicates whether or not the encrypted second content data of interest to the first unit has been received successfully at the first unit; the second communication result indicates whether or not the encrypted first content data of interest to the second unit has been received successfully at the second unit; and the exchange completion data transmission means unit transmits the first exchange completion data to the first unit and the second exchange completion data to the second unit, when the first communication result indicates that the encrypted second content data of interest to the first unit has been received successfully at the first unit and when second communication result indicates

that the encrypted first content data of interest to the second unit has been received successfully at the second unit (Stefik et al., column 54 lines 27-32).

Consider claim 27. Franklin et al., as modified by Boykin et al. and Stefik et al., discloses a computer-readable recording medium having a program recorded thereon, the program for instructing a computer device to exchange, content data of interest that is owned by the computer device with content data of interest to the computer device that is owned by another computer device, the computer device and the other computer device encrypting the content data of interest owned thereby, respectively, when the content data of interest is exchanged therebetween, and the program causing the computer device to execute a method comprising: instructing the computer device to produce first exchange completion data that is a decryption key, and that is necessary for reproducing encrypted content data of interest to the other computer device that is obtained by encrypting the content data of interest to the other computer device that is owned by the computer device; instructing the computer device to register the first exchange completion data produced by the computer device at an exchange completion data keeping device for keeping exchange completion data; and instructing the computer device to obtain, from the exchange completion data keeping device, second exchange completion data that is a decryption key, and that is necessary for reproducing encrypted content data of interest to the computer device that is obtained from the other computer device when a communication session with the other computer device is terminated, wherein the exchange completion data keeping device transmits

(i) the first exchange completion data to the other computer device, and (ii) the second exchange completion data to the computer device, the transmitting of the first and second exchange completion data being performed only when the computer device and the other computer device have successfully received encrypted content data of interest (Franklin et al., column 6 lines 26-34 column and 8 lines 20-44 and column 8 lines 1-8); the computer device and the other computer device, the other computer device encrypting the second content data of interest owned by the other computer device when the second content data of interest is exchanged between the computer device and the other computer device received from the other computer device the encrypted second content data of interest to the computer device and when the other computer device has successfully received from the computer device the encrypted first content data of interest to the other computer device (Stefik et al., column 54 lines 27-32).

Consider claim 28. Franklin et al., as modified by Boykin et al. and Stefik et al., discloses a computer-readable recording medium having a program recorded thereon, the program for instructing a computer device to exchange, content data of interest that is owned by the computer device with content data of interest to the computer device that is owned by another computer device, the computer device and the other computer device encrypting the content data of interest owned thereby, respectively, when the content data of interest is exchanged therebetween, and the program causing the computer device to execute a method comprising instructing the computer device to request an exchange completion data keeping device for keeping exchange completion

data to produce first exchange completion data that is a decryption key, and that is necessary for reproducing encrypted content data of interest to the other computer device that is obtained by encrypting the content data of interest to the other computer device that is owned by the computer device (Franklin et al., column 3 lines 5-15); and instructing the computer device to obtain, from the exchange completion data keeping device, second exchange completion data that is a decryption key, and that is necessary for reproducing encrypted content data of interest to the computer device that is obtained from the other computer device when a communication session with the other computer device is terminated: wherein the exchange completion data keeping device transmits (i) the first exchange completion data to the other computer device, and (ii) the second exchange completion data to the computer device, the transmitting of the first and second exchange completion data being performed only when the computer device and the other computer device have successfully received encrypted content data of interest (Franklin et al., column 8 lines 1-8).

Consider claim 29. Franklin et al., as modified by Boykin et al. and Stefik et al., discloses a computer-readable recording medium having a program recorded thereon, the program for instructing a computer device, which is used in a system for exchanging content data of interest between computer devices connected to each other via a communication medium, to function as: exchange completion data keeping means for keeping exchange completion data that is a decryption key, and that is necessary for reproducing encrypted content data of interest that is encrypted and exchanged

between a first computer device and a second computer device; and exchange completion data transmission means for transmitting exchange completion data that is necessary for reproducing encrypted content data of interest to the first computer device that is obtained by the first computer device to the first computer device and transmitting exchange completion data that is necessary for reproducing encrypted content data of interest to the second computer device that is obtained by the second computer device to the second computer device, the transmitting of the exchange completion data being performed only when the first and second computer devices have successfully received encrypted content data of interest (Franklin et al., column 2 lines 63-67 and column 3 lines 1-15); a first computer device and a second computer device connected to each other via a communication medium, and the program causing the exchange completion keeping device to execute a method comprising: storing first exchange completion data that is a decryption key, and that is necessary for reproducing encrypted second content data of interest to the first computer device that is obtained by the first computer device from the second computer device; obtained by the second computer device from the first computer device (Stefik et al., column 26 line 63 – column 27 line 8); computer device gave has successfully received from the second computer device the encrypted second content data of interest to the first computer device and when the second computer device has successfully received from the first computer device the encrypted first content data of interest to the second computer device (Stefik et al., column 54 lines 27-32).

10. Claims 3, 12, 16, 21, and 24-26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Franklin et al. (US 6263436 B1) in view of Boykin et al. (US 20030079222 A1) in further view of Stefik et al. (US 5629980 A) and in further view of Nagel et al. (US 7181017 B1).

Consider claim 3, as applied to claim 2. Franklin et al., as modified by Boykin et al. and Stefik et al., discloses a method for simultaneous electronic exchange using a semi-trusted third party comprising a unit-to-unit data exchange system.

However, Franklin et al., as modified by Boykin et al., fails to disclose a method of converting data.

Nagel et al. discloses a method for secure three-party communications comprising a first data conversion means for converting the content data of interest to the second unit that is owned by a first unit to encrypted content data of interest to the second unit that can be reproduced successfully only by using a second exchange completion data; and first data recovery means for recovering the content data of interest to the first unit that can be reproduced successfully from encrypted content data of interest to the first unit that is received from a second unit by using first exchange completion data, and wherein the second unit further includes: second data conversion means for converting the content data of interest to the first unit that is owned by the second unit to encrypted content data of interest to the first unit that can be reproduced successfully only by using the first exchange completion data; and second data recovery means for recovering the content data of interest to the second unit that can

be reproduced successfully, from encrypted content data of interest to the second unit that is received from the first unit by using the second exchange completion data (column 5 column 55-67 column 6 lines 1-24).

Therefore, it would have been obvious for a person of ordinary skill in the art at the time the invention was made to incorporate a method of converting data. Nagel et al. discloses a method for secure three-party communications comprising a first data conversion means for converting data owned by a first unit to data that can be reproduced successfully only by using a second exchange completion data; and first data recovery means for recovering data that can be reproduced successfully from data received from a second unit by using first exchange completion data; and the second unit further includes: second data conversion means for converting data owned by the second unit to data that can be reproduced successfully only by using the first exchange completion data; and second data recovery means for recovering data that can be reproduced successfully from data received from the first unit by using the second exchange completion data as taught by Nagel et al. with a method for simultaneous electronic exchange using a semi-trusted third party comprising a unit-to-unit data exchange system as taught by Franklin et al., as modified by Boykin et al., for the purpose of data encryption.

Consider claim 12, as applied to claim 11. Franklin et al., as modified by Boykin et al., Stefik et al., and Nagel et al., further discloses a unit comprising: data conversion means for converting content data of interest to the other unit that is owned by the unit

to encrypted content data of interest to the other unit that can be reproduced successfully only by using the first exchange completion data; and data recovery means for recovering, the content data of interest to the unit that can be reproduced successfully, from encrypted content data of interest to the unit that is (Franklin et al., column 3 lines 16-37) received from the other unit: by using the second exchange completion data obtained by the exchange completion data obtaining means (Nagel et al., 14 12-47).

Consider claim 16, as applied to claim 15. Franklin et al., as modified by Boykin et al., Stezik et al., and Nagel et al., further discloses a unit comprising: conversion process data reception means for receiving conversion process data used for converting the content data of interest to the other unit that is owned by the unit so that the encrypted content data of interest to the other unit to be transmitted to the other unit can be reproduced successfully by using the first exchange completion data sent from the exchange completion data keeping device (Franklin et al., column 3 lines 16-37); data conversion means for converting the content data of interest to the other unit that is owned by the unit by using the conversion process data received by the conversion process data reception means; and data recovery means for recovering, the content data of interest to the unit that can be reproduced successfully from encrypted content data of interest to the unit and obtained from the other unit by using the second exchange completion data obtained by the exchange completion data obtaining means (Nagel et al., 14 12-47).

Consider claim 21, as applied to claim 20. Franklin et al., as modified by Boykin et al., Stefik et al., and Nagel et al., further discloses an exchange completion data keeping device according to claim 20, further comprising conversion process data production/transmission means for (i) producing conversion process data such that exchanged encrypted content data can be reproduced successfully by the first unit and the second unit by using the exchange completion data produced by the exchange completion data production means, and (ii) transmitting the conversion process data to the first unit and the second unit (Nagel et al., column 5 lines 38-67 and column 6 lines 1-24); producing conversion process data such that exchanged the encrypted first content data and the encrypted second content data can be reproduced successfully by the first unit and second unit by using the first exchange completion data and the second exchange completion data produced by the exchange completion data production means unit, and transmitting the conversion process data to the first unit and the second unit (Stefik et al., column 38 lines 23-29, and column 54 lines 27-32).

Consider claim 24, as applied to claim 19. Franklin et al., as modified by Boykin et al., Stefik et al., and Nagel et al., further discloses an exchange completion data keeping device comprising exchange completion data deletion means for deleting exchange completion data kept by the exchange completion data keeping device if a

predetermined condition is satisfied (Nagel et al., column 25 lines 14-44 and column 29 lines 29-41).

Consider claim 25, as applied to claim 24. Franklin et al., as modified by Boykin et al., Stezik et al., and Nagel et al., further discloses an exchange completion data keeping device wherein the predetermined condition is a condition such that the exchange completion data deletion means deletes exchange completion data transmitted to the first and second units from the exchange completion data transmission means if the first unit and the second unit have successfully received the transmitted exchange completion data (Nagel et al., column 25 lines 14-44).

Consider claim 26, as applied to claim 24. Franklin et al., as modified by Boykin et al., Stezik et al., and Nagel et al., further discloses an exchange completion data keeping device wherein the predetermined condition is a condition such that the exchange completion data deletion means deletes the exchange completion data registered by the first unit and the second unit, if the exchange completion data deletion means is notified from either the first unit or the second unit that the encrypted content data of interest has not been received successfully (Nagel et al., column 25 lines 14-44 and column 29 lines 29-41).

Response to Arguments

11. Applicant's arguments filed 03 March 2009 with respect to claims 1, 11, 15, 19 and 27-29 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

12. Any response to this Office Action should be faxed to (571) 273-8300 or mailed to:

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Hand-delivered responses should be brought to

Customer Service Window

Randolph Building
401 Dulany Street
Alexandria, VA 22314

Any inquiry concerning this communication or earlier communications from the Examiner should be directed to Mark Fearer whose telephone number is (571) 270-1770. The Examiner can normally be reached on Monday-Thursday from 7:30am to 5:00pm.

If attempts to reach the Examiner by telephone are unsuccessful, the Examiner's supervisor, Tonia Dollinger can be reached on (571) 272-4170. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status

information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free) or 571-272-4100.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist/customer service whose telephone number is (571) 272-2600.

Mark Fearer
/M.D.F./
June 4, 2009

/George C Neurauter, Jr./
Primary Examiner, Art Unit 2443